Translation

10/525213

PATENT COOPERATION TREATY

PCT/EP2003/008022

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference IP 4537C PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP2003/008022	International filing date (*day/month/year*) 23 July 2003 (23.07.2003)	Priority date (*day/month/year*) 21 August 2002 (21.08.2002)
International Patent Classification (IPC) or national classification and IPC G06F 1/00		
Applicant AUDI AG		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand 17 March 2003 (17.03.2003)	Date of completion of this report 20 December 2004 (20.12.2004)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP2003/008022

I. Basis of the report

1. With regard to the elements of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1, 4-9, as originally filed
pages _____, filed with the demand
pages 2, 3, filed with the letter of 29 July 2004 (29.07.2004)

☒ the claims:

pages _____, as originally filed
pages _____, as amended (together with any statement under Article 19
pages _____, filed with the demand
pages 1-7, filed with the letter of 01 December 2004 (01.12.2004)

☒ the drawings:

pages 1/4-4/4, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed
pages _____, filed with the demand
pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
☐ the language of publication of the international application (under Rule 48.3(b)).
☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.
☐ filed together with the international application in computer readable form.
☐ furnished subsequently to this Authority in written form.
☐ furnished subsequently to this Authority in computer readable form.
☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-7	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-7	NO
Industrial applicability (IA)	Claims	1-7	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following documents:

D1: EP-A-1 197 826 (TOKYO SHIBAURA ELECTRIC CO)
17 April 2002 (2002-04-17)

D2: US 6,378,072 (COLLINS T. ET AL.)
23 April 2002 (2002-04-23)

1. The present application does not meet the requirements of PCT Article 33(1) because the subject matter of claims 1 and 7 does not involve an inventive step within the meaning of PCT Article 33(3).

1.1 The indicated technical problem addressed by the present application is that of providing a process for protecting a motor vehicle control device from interference, in which a memory chip cannot be replaced and data held on the memory chip modified without affecting the functional ability of the motor vehicle control device (see the description, page 2, lines 1-6).

1.2 However, the fact that the present application pertains to a motor vehicle control device cannot be

considered a special technical feature, does not contribute to solving the above-indicated problem and therefore in no way restricts the field of application.

1.3 Therefore, in order to evaluate the closest prior art, a person skilled in the art would consider all documents pertaining to the securing of electronic devices against unauthorized interference with memory chips.

1.4 D1 discloses a process for protecting such a device (in this case a portable memory card). The problem addressed by the invention described in D1 is that of providing a process for protecting such a device from interference, in which undesired memory chip modifications are prevented. For example, not even the owner can replace a memory chip without affecting the functional ability of the device. An encoding process that uses a component-specific identifier of a second component of the device as the key initially encodes data that are later stored in a reversible memory chip.

D1 is considered to represent the closest prior art in relation to the subject matter of claim 1.

1.5 In particular, D1 discloses (the references in parentheses are to this document) a process for protecting a device from interference (see column 1, lines 18-24), wherein the device comprises a microcomputer and memory chips (see column 3, lines 42-45; column 4, lines 16-19; figure 17) and the memory chips constitute a reversible read-only storage device (see embodiment 4, column 8, lines

48-50), characterized in that data that have been encoded by an encoding process (see column 9, line 8) are stored in the reversible read-only storage device (see column 9, lines 13-14) and the key used in the encoding process consists of the component-specific identifier of a component ("*unique encoding key ... stored beforehand*"; see column 8, lines 27-28; column 9, lines 9-10).

1.6 The subject matter of claim 1 thus differs from that of D1 in that the present application pertains to a motor vehicle control device. However, this feature cannot be considered a special technical feature, does not contribute to solving the above-indicated problem and therefore in no way restricts the field of application. Claim 1 therefore does not involve an inventive step within the meaning of PCT Article 33(3).

1.7 The same reasoning applies *mutatis mutandis* to independent claim 7. The subject matter of claim 7 therefore does not involve an inventive step within the meaning of PCT Article 33(3).

2. Dependent claims 2-6 do not contain any features which, in combination with the features of any claim to which they refer back, meet the PCT requirements for inventive step.

2.1 **Claims 2 and 3**. The subject matter of claims 2 and 3 is likewise known from D1, since the identifier used in the encoding process may be considered as both an identifier of the microcomputer (memory chip *internal memory 3b* regarded as an internal component of the microcomputer) and an identifier of a further

memory chip.

2.2 **Claim 4**. The feature of storing the key in the RAM of the microcomputer is a conventional measure. Inclusion of this measure in D1 in order to use the encoding process would represent an obvious, routine technical approach to solving the problem of interest to a person skilled in the art.

2.3 **Claim 5**. The subject matter of claim 5 is known from D1 because the identifier is read out from a read-only area of the microcomputer (see D1, column 8, lines 30-41).

2.4 **Claim 6**. In D1, in contrast to claim 6, the key is read out randomly from a memory chip and used directly for data decoding (see column 9, lines 7-12 and 20-23). The subject matter of claim 6 thus differs from that of D1 in that, whenever the control device is actuated, a key for decoding data is newly generated. The problem addressed by the present invention may therefore be considered that of improving the security of the key for decoding data.

This feature is only one of several obvious possibilities from which a person skilled in the art would choose according to the circumstances in order to solve the problem of interest, without thereby being inventive. The key may, for example, either be read out randomly or newly generated from multiple components or by specific algorithms. D2 (see page 8, lines 48-53) describes the same advantages with respect to this feature as does the present application. A person skilled in the art would

therefore consider inclusion of this feature in the subject matter of D1 to be a routine design step and the solution proposed in claim 6 of the present application cannot, therefore, be considered to involve an inventive step (PCT Article 33(3)).

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts IP 4537C PCT	**WEITERES VORGEHEN** siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP 03/08022	Internationales Anmeldedatum *(Tag/Monat/Jahr)* 23.07.2003	Prioritätsdatum *(Tag/Monat/Jahr)* 21.08.2002
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G06F1/00		
Anmelder AUDI AG		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Bescheids
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Regel 66.2 a)ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
17.03.2004	20.12.2004
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter Sigolo, A Tel. +31 70 340-4173

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP 03/08022

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17))*:

Beschreibung, Seiten

1, 4-9	in der ursprünglich eingereichten Fassung
2, 3	eingegangen am 29.07.2004 mit Schreiben vom 26.07.2004

Ansprüche, Nr.

1-7	eingegangen am 01.12.2004 mit Schreiben vom 25.11.2004

Zeichnungen, Blätter

1/4-4/4	in der ursprünglich eingereichten Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um:

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).

   ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).

   ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

   ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

   ☐ Beschreibung, Seiten:

   ☐ Ansprüche, Nr.:

   ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen.)

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-7
	Nein:	Ansprüche	
Erfinderische Tätigkeit (IS)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-7
Gewerbliche Anwendbarkeit (IA)	Ja:	Ansprüche:	1-7
	Nein:	Ansprüche:	

2. Unterlagen und Erklärungen:

   siehe Beiblatt

Zu Punkt V

Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf die folgenden Dokumente verwiesen:
D1: EP-A-1 197 826 (TOKYO SHIBAURA ELECTRIC CO) 17. April 2002 (2002-04-17)
D2: US 6,378,072 (COLLINS T. ET AL.) 23. April 2002 (2002-23-04)

1. Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33(1) PCT, weil der Gegenstand der Ansprüche 1 und 7 nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3) beruht.

1.1 Die angegebene technische Aufgabe der vorliegenden Anmeldung ist es, ein Verfahren zum Schutz vor Manipulation an einem Fahrzeug-Steuergerät zu schaffen, bei dem ein Austausch eines Speicherbausteins und die Änderung der Daten auf dem Speicherbaustein nicht möglich ist, ohne die Funktionsfähigkeit des Fahrzeug-Steuergeräts zu beeinflussen (siehe Beschreibung, Seite 2, Zeilen 1-6).

1.2 Die Tatsache, dass es sich um ein Fahrzeug-Steuergerät handelt, kann aber nicht als besonderes technisches Merkmal angesehen werden, trägt nicht zur Lösung der obengenannten Aufgabe bei und engt deshalb in keiner Weise den technischen Anwendungsbereich ein.

1.3 Um den nächstliegenden Stand der Technik zu beurteilen, würde der Fachmann deshalb alle Dokumente berücksichtigen, die die Sicherung elektronischer Geräte gegen unerlaubte Manipulation der Speicherbausteine behandeln.

1.4 D1 offenbart ein Verfahren zum Schutz eines solchen Geräts, hier in Form einer tragbaren Speicherkarte. Aufgabe der Erfindung von D1 ist es, ein Verfahren zum Schutz vor Manipulation an einem solchen Gerät zu schaffen, bei dem unerwünschte Veränderungen der Speicherbausteine verhindert werden. Beispielweise ist es nicht möglich, nicht einmal für den Besitzer, einen Speicherbaustein auszutauschen, ohne die Funktionsfähigkeit des Geräts zu beeinflussen. Dazu werden zuerst die Daten, die später auf einem reversiblen Speicherbaustein abgelegt werden, durch ein Verschlüsselungsverfahren, das eine bausteinspezifische Kennung eines zweiten

Bausteins des Geräts als Schlüssel verwendet, verschlüsselt.

D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 1 angesehen.

1.5 Insbesondere offenbart D1 (die Verweise in Klammern beziehen sich auf dieses Dokument) ein Verfahren zum Schutz vor Manipulation eines Geräts (siehe Spalte 1, Zeilen 18-24), wobei das Gerät einen Microrechner und Speicherbausteine umfasst (siehe Spalte 3, Zeilen 42-45; Spalte 4, Zeilen 16-19; Abbildung 17), und die Speicherbausteine einen reversiblen Festwertspeicher darstellen (siehe das Ausführungsbeispiel 4, Spalte 8, Zeilen 48-50), dadurch gekennzeichnet, dass in den reversiblen Festwertspeicher Daten abgelegt werden (siehe Spalte 9, Zeilen 13-14), die durch ein Verschlüsselungsverfahren verschlüsselt worden sind (siehe Spalte 9, Zeile 8), und der in dem Verschlüsselungsverfahren verwendete Schlüssel aus der bausteinspezifische Kennung eines Bausteins besteht ("*unique encoding key ... stored beforehand*" siehe Spalte 8, Zeilen 27-28; Spalte 9, Zeilen 9-10).

1.6 Der Gegenstand des Anspruchs 1 unterscheidet sich daher von dem bekannten D1 dadurch, daß es in der vorliegenden Anmeldung um ein Fahrzeug-Steuergerät handelt. Dieses Merkmal kann aber nicht als besonderes technisches Merkmal angesehen werden, trägt nicht zur Lösung der obengenannten Aufgabe bei und engt deshalb in keiner Weise den technischen Anwendungsbereich ein. Deshalb beruht Anspruch 1 nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3).

1.7 Die gleiche Begründung gilt entsprechend für den unabhängigen Anspruch 7. Der Gegenstand des Anspruchs 7 beruht daher nicht auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).

2. Die abhängigen Ansprüche 2 zu 6 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in bezug auf erfinderische Tätigkeit erfüllen.

3.1 **Ansprüche 2 und 3**. Der Gegenstand der Ansprüche 2 und 3 ist ebenfalls aus D1 bekannt, da die in dem Verschlüsselungsverfahren verwendete Kennung sowohl als eine Kennung des Microrechners (der Speicherbaustein *internal memory 3b* als ein betriebsinteres Bauelement des Microrechners angesehen) als auch als eine Kennung eines weiteren Speicherbausteins betrachtet werden kann.

3.2 **Anspruch 4**. Das Merkmal, den Schlüssel in dem RAM des Microrechners abzulegen, ist eine fachübliche Maßnahme. Um das Verschlüsselungverfahren einzusetzen, wäre die Aufnahme dieser Maßnahme in Dokument D1 für den Fachmann eine naheliegende, im Rahmen normalen fachlichen Handelns liegende Vorgehensweise zur Lösung der gestellten Aufgabe.

3.3 **Anspruch 5**. Der Gegenstand des Anspruchs 5 ist aus D1 bekannt, weil die Kennung aus einem lesegeschützten Bereich des Microrechners ausgelesen wird (siehe D1, Spalte 8, Zeilen 30-41).

3.4 **Anspruch 6**. In Dokument D1 wird der Schlüssel hingegen aus einem Speicherbaustein willkürlich ausgelesen und direkt zum Datenentschlüsseln verwendet (siehe Spalte 9, Zeilen 7-12 und 20-23). Der Gegenstand des Anspruchs 1 unterscheidet sich daher vom bekannten D1 dadurch, dass bei jeder Inbetriebnahme des Steuergeräts ein Schlüssel zum Entschlüsseln der Daten neu erzeugt wird. Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, dass man die Sicherheit des Schlüssels zum Entschlüsseln der Daten erhöhen will.

Bei diesem Merkmal handelt es sich nur um eine von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde, um die gestellte Aufgabe zu lösen. Der Schlüssel kann zum Beispiel entweder willkürlich ausgelesen werden, oder aus mehreren Komponenten oder durch speziefische Algorithmen neu erzeugt werden. Dokument D2 (siehe Seite 8, Zeilen 48-53) beschreibt hinsichtlich dieses Merkmals dieselben Vorteile wie die vorliegende Anmeldung. Der Fachmann würde daher die Aufnahme dieses Merkmals als eine übliche konstruktive Maßnahme im Gegenstand von D1 und deshalb kann die in Anspruch 1 der vorliegenden Anmeldung vorgeschlagene Lösung nicht als erfinderisch betrachtet werden (Artikel 33(3) PCT).

Aufgabe der vorliegenden Erfindung ist es daher, ein Verfahren zum Schutz vor Manipulation an einem Steuergerät zu schaffen, bei dem ein Austausch eines Speicherbausteins und die Änderung der Daten auf dem Speicherbaustein nicht möglich ist, ohne die Funktionsfähigkeit des Steuergeräts zu beeinflussen oder zumindest die Veränderung zu diagnostizieren und diese ggf. zur Anzeige zu bringen.

Der Erfindung liegt die Erkenntnis zugrunde, dass diese Aufgabe gelöst werden kann, indem eine Verschlüsselung der Daten, die auf einem Speicherbaustein abgelegt sind, verwendet wird, die ausschließlich von dem dem Speicherbaustein ursprünglich zugeordneten Microrechner entschlüsselt werden kann.

Die Aufgabe wird daher gelöst durch ein Verfahren zum Schutz vor Manipulation eines Steuergeräts für mindestens eine Kfz-Komponente, wobei das Steuergerät zumindest einen Microrechner und mindestens einen Speicherbaustein umfasst, wobei zumindest einer der Speicherbausteine einen reversiblen Festwertspeicher darstellt, dadurch gekennzeichnet, dass, in den reversiblen Festwertspeicher Daten abgelegt werden, die durch ein Verschlüsselungsverfahren verschlüsselt worden sind, und der in dem Verschlüsselungsverfahren verwendete Schlüssel zumindest einen Teil mindestens einer ursprünglichen bausteinspezifischen Kennung mindestens eines der Bausteine des Steuergeräts umfasst, *

Durch das Integrieren zumindest eines Teils der spezifischen Kennung mindestens einer der ursprünglich in dem Steuergerät eingesetzen Bausteine des Steuergeräts kann eine sinnvolle Entschlüsselung nur von dem Microrechner aus erfolgen, der ursprünglich dem Speicherbaustein zugeordnet war. Ein Austauschen des reversiblen Speicherbausteins, der beispielsweise ein EEPROM darstellen kann, mit den dazugehörigen Daten ist daher nicht möglich.

Vorzugsweise stellt die Kennung, die in dem Schlüssel zum Entschlüsseln der Daten, die auf dem Festwertspeicher gespeichert sind, verwendet wird, eine Kennung des Microrechners dar. Vorzugsweise ist diese Kennung die Identifikationsnummer, die bei der Herstellung des Microrechners vergeben und in diesem abgelegt wird.

* wobei bei jeder Inbetriebnahme des Steuergerätes ein Schlüssel zum Entschlüsseln der in den reversiblen Festspeicher verschlüsselt abgelegten Daten neu erzeugt wird.

Zusätzlich oder alternativ kann die Kennung aber auch eine Kennung eines weiteren Speicherbausteins des Steuergeräts darstellen. So kann beispielsweise die Identifikationsnummer eines mit dem Microrechner verbundenen oder in diesem integrierten Flash-Speichers als Kennung dienen. Dadurch wird der Austausch einzelner Bauteile des Steuergeräts noch weiter erschwert.

Um das Auslesen des Schlüssels, der zumindest teilweise die ursprünglichen Kennungen zumindest eines Teils der Bausteine des Steuergeräts umfasst, zu vermeiden, kann der Schlüssel in dem RAM des Microrechners abgelegt werden. Diese Ausführungsform ist insbesondere ~~dann~~ zu bevorzugen, ~~wenn~~ da bei jeder Inbetriebnahme des Steuergeräts der Schlüssel zum Entschlüsseln der in dem reversiblen Festspeicher verschlüsselt abgelegten Daten neu erzeugt wird ~~werden soll~~. Dieses Erzeugen des Schlüssels gewährt eine zusätzliche Sicherheit gegen den Austausch einzelner Komponenten des Steuergeräts.

Vorzugsweise wird zur Erzeugung eines Schlüssels zum Entschlüsseln von Daten auf einem reversiblen Festwertspeicher aus einem lesegeschützten, nur einmalig beschreibbaren (one-time-programmable) OTP-Bereich des Microrechners mindestens ein Teil einer Kennung mindestens eines der Bausteine des Steuergeräts ausgelesen.

Die Erfindung wird im Folgenden anhand der beiliegenden Zeichnungen, die sich auf mögliche Ausführungsbeispiele der Erfindung beziehen, beschrieben. Es zeigen:

Figur 1 und 1a: Flußdiagramme, die den Verlauf des erfindungsgemäßen Verfahrens schematisch wiedergeben;

Figur 2: eine schematische Blockdarstellung einer Ausführungsform eines Steuergeräts zum Ausführen des erfindungsgemäßen Verfahrens; und

Figur 3: eine schematische Blockdarstellung einer weiteren Ausführungsform eines Steuergeräts zum Ausführen des erfindungsgemäßen Verfahrens.

In Figur 1 ist der Ablauf des erfindungsgemäßen Verfahrens schematisch in einem Flußdiagramm angedeutet und wird im folgenden erläutert.

IP 4537C
Pz

Patentansprüche

1. Verfahren zum Schutz vor Manipulation eines Fahrzeug-Steuergeräts, wobei das Fahrzeug-Steuergerät (1) zumindest einen Mikrorechner (μC) und mindestens einen Speicherbaustein (2, 3) umfasst, wobei zumindest einer der Speicherbausteine (2, 3) einen reversiblen Festwertspeicher (3) darstellt, dadurch gekennzeichnet, dass in den reversiblen Festwertspeicher (3) Daten abgelegt werden, die durch ein Verschlüsselungsverfahren verschlüsselt worden sind, und der in dem Verschlüsselungsverfahren verwendete Schlüssel zumindest einen Teil mindestens einer ursprünglichen bausteinspezifischen Kennung (ID) mindestens eines der Bausteine (μC, 2, 3) des Steuergeräts umfasst.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, dass die Kennung eine Kennung des Mikrorechners (μC) darstellt.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Kennung eine Kennung eines weiteren Speicherbausteins (3) darstellt.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Schlüssel in dem RAM des Mikrorechners (μC) abgelegt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zur Erzeugung eines Schlüssels zum Verschlüsseln von Daten auf einem reversiblen Festwertspeicher (3) aus einem lesegeschützten OTP-Bereich (11) des Mikrorechners mindestens ein Teil einer Kennung (ID) mindestens eines der Bausteine (μC, 2, 3) des Steuergeräts (1) ausgelesen wird.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass bei jeder Inbetriebnahme des Steuergeräts (1) ein Schlüssel zum Entschlüsseln der in dem reversiblen Festspeichers (3) verschlüsselt abgelegten Daten neu erzeugt wird.

7. Fahrzeug-Steuergerät, in dem ein Verfahren nach einem der Ansprüche 1 bis 6 realisiert ist.